

## DATA SHEET

# Taegis™ XDR

Expect more from XDR. Secureworks® delivers security and visibility beyond your expectations, mitigating threats and harnessing the power of advanced security analytics, automated detection engines, and decades of unique human threat intelligence and cybersecurity expertise.

## Outpace and Outmaneuver Your Adversaries

Cyber-attacks and threats have never been more aggressive, sophisticated, or stealthy. Their impact is leaving too many businesses and government organizations struggling to maintain and strengthen their defenses. Facing limited visibility into their dispersed IT environments, understaffed security teams, and the growing cost and complexities of managing disparate security tools, many organizations are looking to XDR (Extended Detection and Response) as a way of unifying their existing IT security infrastructures. With XDR, organizations can rely on a single SecOps investigation and response platform to help them manage and rapidly respond to threats, with time-saving automation that helps achieve better security and risk reduction outcomes.

Secureworks Taegis™ XDR cloud-native SaaS platform is designed to exceed your expectations. Taegis XDR improves the effectiveness and efficiency of your security operations by incorporating in-depth security knowledge of the threat landscape that has made Secureworks a security leader for over 22 years.

- Gain holistic visibility and control over your Windows, macOS and Linux endpoint, network, and cloud environments by aggregating real-time telemetry from across your organization's IT environments.
- Detect advanced threats and MITRE ATT&CK TTPs with AI-powered analytics, thousands of built-in automated countermeasures, a family of machine learning threat detectors and powerful Tactic™ Graphs to connect related low-level events. All features built into Taegis are constantly enriched for you with comprehensive threat intelligence inputs from the Secureworks Counter Threat Unit™ and thousands of real-world Incident Response engagements that our Secureworks team has completed.
- Accelerate investigations by focusing in on high and critical alerts. Taegis supplies you incident response data and threat-hunting tools, plus automated playbooks at your fingertips in one easy-to-use cloud console.

---

## Key Capabilities

- Comprehensive attack surface coverage including endpoint, network, and cloud environments
- Machine and deep learning-driven analyses of telemetry and events from multiple attack vectors enriched with comprehensive threat intelligence
- High-fidelity alerts augmented with all the context and data you need, when and where you need them
- Single-click response actions and automated playbooks
- An open XDR solution offers extensive pre-built and easy-to-create custom integrations with 3rd-party security tools

## Why Taegis XDR

### Superior Detection

Superior detection comes from having the ability to use at scale highly accurate and relevant data, and then to apply a wide range of automated detection and detectors to uncover real-time threats, and involve skilled human expertise as needed.

From a data perspective the Taegis XDR data lake processes over 47BN events per day with over 60% of those events coming from non-endpoint sources. Taegis XDR supercharges detection by applying threat intelligence insights from the three thousand plus incident response and penetration testing engagements undertaken every year, plus over 55,000 annual threat hunts!

Further security intelligence comes from our in-house Threat Intelligence team tracking 175+ global threat groups and who work alongside our in-house Counter Threat Unit to help maintain, update and keep relevant over 600,000 threat indicators and 20,000+ built-in Taegis XDR countermeasures.

With daily inputs and the use of many advanced and propriety AI/Machine Learning detectors it's easy to see how Taegis XDR covers the MITRE ATT&CK framework and offers truly battle-ready and superior threat detection.

### Unmatched Response

When things are uncertain and immediate security expertise is needed Taegis XDR provides and includes for every customer 60 seconds or less access to a security expert in our SOC. With the Taegis XDR platform console (purposely developed and designed for collaboration) rapid response and detailed investigation is immediate.

Taegis XDR also incorporates 70+ proprietary automated playbooks powered by our knowledge and decades of SecOps expertise. Expertise that is validated by Secureworks being one of a handful of security companies accredited to work with the US and UK governments on critical national infrastructure events.

And from our customers' perspective offering a fully in-house "event to resolution" customer partnership that covers additional support areas like Adversarial Testing; SOC; Threat Research; Incident Response and Investigations - all from a recognized leader in MDR (M-XDR according to Forrester & IDC).

### Open without Compromise Platform

Our open Taegis XDR platform helps our customers avoid vendor 'lock-in' as it supports many and a growing number of major security solutions. Taegis XDR was designed from the ground up to be 'vendor neutral' and we now offer well over 100 integrations. Openness stretches to our customer partnership models too. You can deploy Taegis XDR as your in-house software security operations solution, or choose to work with Secureworks, one of our Taegis Partners, or choose from our different levels of Managed XDR service offerings.

### Higher ROI

Customers who have chosen Secureworks have seen ~400% ROI on their investment. Apart from unifying your security tools, and creating a highly efficient and effective security operations environment, Taegis XDR is successful at displacing and recovering wasted SIEM data retention costs and investments in technologies that are now included in Taegis XDR at no extra cost.

Taegis XDR also removes concerns about cost of operation and budgeting predictability by using a straightforward and inclusive SaaS per-endpoint pricing for all versions of Taegis XDR. For instance, Taegis XDR includes 12 months rolling data retention of all log data as standard. And by reducing MTTR (Mean Times to Respond) through high priority response action recommendations and automated playbooks customers see security incident costs minimized.

## Maximize Security Effectiveness

### Prevent, Detect and Respond to Known and Unknown Threats

- Endpoints are often the first line of defense for many organizations. Taegis XDR combines powerful next-generation endpoint prevention capabilities of Taegis NGAV with rich endpoint telemetry with rich near real-time endpoint telemetry from the Taegis (EDR) agent. Consequently, you can disrupt most threats that appear in your endpoint environments, while enriching threat investigations with additional endpoint context
- Taegis XDR aggregates signals from your network, cloud, endpoint and other security tools with curated threat intelligence, so you can gain full visibility and control over your entire attack surface
- Taegis AI-powered detectors leverage state-of-the-art machine learning algorithms and analytical techniques to continuously monitor your environment for malicious activity, recognizing adversarial behavior early on. Taegis XDR automatic playbooks and single-click response actions enable rapid response. Taegis is designed to help you can detect, understand, and stop sophisticated attacks before they can do the damage

### Understand Threat Actors' Intent and Behavior

- Comprehensive threat intelligence continuously produced by the Secureworks Counter Threat Unit provides in-depth analysis of emerging threats and threat actor intent and behavior. Taegis XDR countermeasures incorporate this knowledge to disrupt attacks. Plus, your teams can use this knowledge to fully understand etc.

## Boost SecOps Efficiency

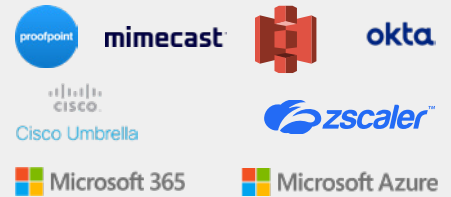
### Investigate What Matters

- With comprehensive coverage of your organization's security fabric, Taegis correlates threat intelligence, logs and events from different security tools to validate and prioritize alerts. As a result, your analysts spend less time dealing with false positives and more time addressing real threats

### Solve the Attack Puzzle Faster

- Taegis automatically correlates related events across your endpoint, network, and cloud environments to help you gain a full understanding of the threat scenario and quickly determine the root cause of an attack

Taegis XDR is an open platform able to integrate 100's of your existing security tools.



## boohoo

[Global Retailer Slashes Risk With Secureworks](#)

**“Secureworks brings a scale we can’t achieve alone and can spot things that we might overlook. That’s what we have experienced with some threats Secureworks has detected.”**

—Ewan Osborne, Cyber Security Analyst

[Global Aviation Manufacturer](#)

**“Secureworks helps me extend my department beyond its actual size. This solution has doubled our effectiveness. So we are leveraging the people and services at Secureworks every day.”**

—IT Risk & Compliance Manager



### Perform All Investigations in One Platform

- Taegis collects data from across your environment and incorporates a comprehensive threat-hunting toolkit, including MITRE ATT&CK TTPs. Accordingly, your analysts get a full view of your security infrastructure and can perform all investigations within the platform, without having to manually stitch data or bounce between tools

### Reduce Risks by Blocking Threats at the Endpoint

- Taegis NGAV is designed to stop most attacks on the endpoint automatically, including targeted and novel attacks, reducing the risk of breach while decreasing the volume of threats that must be investigated. Consequently, this may lead to fewer threats breaking through your endpoints and analysts can focus on more advanced and critical threats

### Work Smarter and Faster Together

- With more flexible search and reporting capabilities, your analysts can assemble relevant information quickly and share it with others on your team to collaborate on investigations: make comments, add or remove related data, and change status. This way, you can accelerate investigations via improved collaboration and faster decision-making

### Gain Immediate Access to Secureworks Experts

- Whenever you or your analysts have questions about security alerts, workflows, or need help with investigations, you can reach a Secureworks expert in as quickly as 60 seconds directly from the Taegis console.




*“Taegis NGAV is a mature product, ready to be used in a wide set of deployment scenarios, ranging from small environments to multinational enterprises.”*

*“With its solid performance, convincing detection capabilities against in-the-wild malware, SOC-ready console and feature set, Secureworks Taegis NGAV is a trustworthy addition to any IT security arsenal.”*

---

**MRG Effitas Efficacy  
Assessment Report**

# Secureworks Taegis XDR Highlights



**20+**  
Years of Secureworks' leadership in security services and threat research

**175+**  
Threat groups monitored by Secureworks

**60 seconds or less**  
To reach a Secureworks experts when you need help with an investigation

**~98%**  
Around 98% of [MITRE ATT&CK TTPs](#) Covered

*"We generate around 2 billion events each month. With Secureworks, we are able to crunch down that number to 20-30 high fidelity alerts—and that makes my team's job much easier."*

---

**Sunil Saale, Head of Cyber and Information Security, MinterEllison**

## System Requirements

### Taegis XDR Console

As a cloud native application you need a modern browser:

- Chrome
- Edge
- Firefox

Mobile web browsers are not supported at this time.

### Supported Systems Taegis XDR Agent

#### Microsoft Windows:

- Windows 10, 11
- Windows Server 2016, 2019 and 2022

#### macOS:

- MacOS Catalina 10.15
- Big Sur 11
- Monterey 12 (+M1)

#### Other:

- CentOS 7
- Amazon Linux 2
- Ubuntu 18.04

You can find more information on our [Taegis XDR Documentation Site](#)

### About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.



For more information, call **1-877-838-7947** to speak to a Secureworks security specialist [secureworks.com](https://secureworks.com)